On the ring of local polynomial invariants for a pair of entangled qubits

V. Gerdt [a], A. Khvedelidze [a,b], and Yu. Palii [a,c]

[a] *Laboratory of Information Technologies, Joint Institute for Nuclear Research, Dubna, 141980, Russia*

[b] *Department of Theoretical Physics, A. Razmadze Mathematical Institute, Tbilisi GE-0193, Georgia*

[c] *Institute of Applied Physics, Chisinau MD-2028, Moldova*

Abstract

The entanglement characteristics of two qubits are encoded in the invariants of the adjoint action of $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$ group on the space of density matrices $\mathfrak{P}_+$, defined as the space of 4×4 positive semi-definite Hermitian matrices. The corresponding ring $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ of polynomial invariants is studied. The special integrity basis for the ring $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$, is described and constraints on its elements due to the positive semi-definiteness of density matrices are given explicitly in the form of polynomial inequalities. The suggested basis is characterized by the property that only a minimal number of invariants, namely two primary invariants of degree 2, 3 and one secondary invariant of degree 4 appearing in the Hironaka decomposition of $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$, are subject to the polynomial inequalities.

1 Introduction

According to the quantum theory non-locality of a quantum word manifests itself in a way that is very different from the intuitive classical views. At the very outset of quantum epoch reflections on that fact create a variety of paradoxes beginning from the Eistein-Podolski-Rosen paradox and the famous neither dead nor alive Schrödinger cat [1, 2, 3]. Only towards the end of the XX-th century after the advances of technology, when a manipulation with quantum coherency became reality, the pragmatic approach to the problem rises the question of a practical usage of quantum non-locality. Time for the realization of quantum communications and creation of the quantum computer has to come [4].

The difference between quantum and classical correlations has a very transparent mathematical background. One can already see its roots comparing the basic states of classical and quantum computers; bits and qubits. While an arbitrary n-bit string can be transformed into other by the so-called "local transformation", acting on its constituent bits, in quantum case this is true for one qubit states only. In other words the action of "local transformation" cease to be *transitive* for multiqubit systems [5, 6]. The action of local transformations splits the space of an arbitrary quantum system into the equivalence classes in way that each class is characterized by a different non-local properties [7]. Therefore the problem of classification of non-localities in a system of n-qubits reduces to the mathematical problem of description of orbits of "local" group action on the space of states [8, 9]. The corresponding orbit space, $\mathcal{E}_n$, is termed as *"entanglement space"* [5, 6]. For its characterization the mathematical formalism based on the classical theory of invariants (c.f. [10, 11]) is often applied. In this approach, in order to separate orbits, i.e., to introduce coordinates on $\mathcal{E}_n$, the polynomials in elements of the density matrices, which are invariant under the local transformation, are used.

The entanglement space has highly nontrivial geometric and topological structure [6, 12]. Especially, a complexity of $\mathcal{E}_n$ is steeply rising with number of qubits growing up. This makes computations very tedious. However, for the lowest, 2-qubits system, the approach based on the classical theory of invariants allows to obtain a series of important algebraic results, clarifying the properties of $\mathcal{E}_2$ [9, 13, 14].

There is one further complication with the description of $\mathcal{E}_n$. In virtue of a physical requirement the density matrices should be positive semi-definite

[15, 16, 17]. Therefore, the space of local group action is not a linear space, but represents a certain semi-algebraic variety $\mathfrak{P}_+$. This circumstance should be taken into account applying the classical theory of invariants for construction of the orbit space. In the present article this problem is analyzed and detailed solution is given for the case of 2-qubits. With this aim the semi-definiteness of density matrices is formulated explicitly in the form of polynomial inequalities in the scalars of the adjoint action of the group $\mathrm{SU}(2) \otimes \mathrm{SU}(2)$. Apart from this, the integrity basis for the polynomial ring $\mathbb{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes \mathrm{SU}(2)}$, that includes the minimal number of elements subject to the above inequalities, will be presented.

Our plan is as follows. We start, in paragraphs 2 and 3, with the brief review of necessary notions from quantum mechanics and put them into context suitable for the characterization of entanglement within the classical theory of invariants. Further, in the 4-th paragraph the system of polynomial inequalities in the Casimir operators of enveloping algebra of $\mathrm{SU}(4)$, that describes the space $\mathfrak{P}_+$ is derived. Regarding to these inequalities, in the last paragraph the integrity basis for the ring $\mathbb{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes \mathrm{SU}(2)}$ is constructed.

2 The space of states

A generic mixed state of n-level quantum system is described by $n \times n$ complex matrix, the density matrix ϱ [15, 16], satisfying following conditions[1]:

i. *Hermicity* $- \varrho = \varrho^+$,

ii. *finite trace* $- \mathrm{Tr}(\varrho) = 1$,

iii. *positive semi-definiteness* $- \varrho \geq 0$.

Mixed states form the subspace $\mathfrak{P}_+$, of the space of Hermitian $n \times n$ matrices. It is instructive, before considering a generic n-level system, to start with the simplest two-level quantum mechanical model.

[1]The special class of idempotent matrices, $\varrho^2 = \rho$, corresponds to the so-called *pure states*, whose description reduces to the usage of rays in a Hilbert space. A mixed state is a mixture of pure states.

2.1 Qubit

In quantum theory of information an abstract quantum mechanical model with two levels takes a special place and independently of its physical realization carries the universal name – *qubit*.

The qubit state is given by a density matrix that coincides with the standard density matrix of the non-relativistic spin 1/2:

$$\varrho = \frac{1}{2}\,(1 + \boldsymbol{\alpha}\cdot\boldsymbol{\sigma})\;, \tag{1}$$

where $\boldsymbol{\sigma}$ - set of the Pauli matrices [2] and $\boldsymbol{\alpha}$ is defined as mathematical expectation:

$$\boldsymbol{\alpha} = \mathrm{Tr}\,(\boldsymbol{\sigma}\varrho)\;,$$

In the representation (1) requirements (i.) and (ii.) are taken into account by construction. The condition (iii.) restricts the parameter space of mixed states by a unit ball

$$\boldsymbol{\alpha}^2 \le 1\,, \tag{2}$$

while for the pure states of qubit the expectation $\boldsymbol{\alpha}$ lies on the Bloch 2-sphere

$$\boldsymbol{\alpha}^2 = 1\,.$$

2.2 Qudit

Analogously to the qubit the special terminology for d - level quantum system, a *"qudit"*, has been introduced. The generalization of representation (1) to the case of qudits reads [18]:

$$\varrho = \frac{1}{d}\left(\mathbb{I}_d + \sqrt{\frac{d(d-1)}{2}}\,\boldsymbol{\xi}\cdot\boldsymbol{\lambda}\right)\;, \tag{3}$$

where $\boldsymbol{\xi} = \langle\boldsymbol{\lambda}\rangle \in \mathbb{R}^{d^2-1}$ is d^2-1- dimensional Bloch vector. In the expansion (3) components of the vector $\boldsymbol{\lambda} = (\lambda_1, \lambda_2, \dots, \lambda_{d^2-1})$ represent the elements of the su(d) algebra normalized by conditions

$$\lambda_i\lambda_j = \frac{2}{d}\,\delta_{ij}\mathbb{I}_d + (d_{ijk} + i\,f_{ijk})\lambda_k,$$

[2] The explicit form of σ-matrices is given below, in paragraph 5, formulaes (18).

δ_{ij} is the Kronecker symbol. The constants d_{ijk} and f_{ijk} are the so-called totally symmetric and antisymmetric structure constants of the algebra:

$$d_{abc} = \frac{1}{4}\mathrm{Tr}(\{\lambda_a, \lambda_b\}\lambda_c), \qquad f_{abc} = -\frac{i}{4}\mathrm{Tr}([\lambda_a, \lambda_b]\lambda_c),$$

where

$$\{\lambda_a, \lambda_b\} = \lambda_a\lambda_b + \lambda_b\lambda_a, \qquad [\lambda_a, \lambda_b] = \lambda_a\lambda_b - \lambda_b\lambda_a.$$

As for the case of a qubit, the properties (i.) and (ii.) of the qudit's density matrix are already taken into account in the decomposition (3). The non-negativity requirement (iii.) imposes further, more subtle than (2), restrictions. A complete characterization of qudit's Bloch vector space, $\mathbf{B}(\mathbb{R}^{d^2-1})$, in an arbitrary dimension, is an open problem. However, some general properties of this space is already known. Particularly, it can be shown that $\mathbf{B}(\mathbb{R}^{d^2-1})$ is a convex subset of a d^2-1-dimensional unit ball

$$\boldsymbol{\xi}^2 \leq 1\,.$$

It being know that all pure states are concentrated on its surface. More precisely, qudit's pure states are determined by the equation

$$\boldsymbol{\xi}^2 = 1\,, \qquad \boldsymbol{\xi} \vee \boldsymbol{\xi} = \boldsymbol{\xi}\,,$$

where

$$(\boldsymbol{\xi} \vee \boldsymbol{\xi})_k := \sqrt{\frac{d(d-1)}{2}}\,\frac{1}{d-2}\,d_{ijk}\xi_i\xi_j\,.$$

2.3 Composite states

From the standpoint of quantum information theory it is mostly interesting to consider states composed of several qubits. According to the quantum theory axiom on composite systems [4], the space of states of system, which is obtained by joining two systems A and B, represents a subspace of the tensor product of their individual Hilbert spaces $\mathcal{H}_A$ and $\mathcal{H}_B$:

$$\mathcal{H} \subset \mathcal{H}_A \otimes \mathcal{H}_B\,. \tag{4}$$

The definition (4) in conjunction with the superposition principle is a source of an existence of correlations in the joint system, which do not have

any classical analog. If a mixed state ϱ, describing the joint $A+B$ system, admit (not necessary in unique way) representation of the form

$$\varrho = \sum_{j=1}^{M} \omega_j \, \varrho_j^A \otimes \varrho_j^B \,, \qquad \omega_j > 0\,, \qquad \sum_{j=1}^{M} \omega_j = 1\,, \tag{5}$$

where ϱ_j^A and ϱ_j^B are density matrices of subsystems, then this joint state is called *separable* [7]. For such a state correlations between subsystems are classically conceivable. But the states (5) are far to exhaust all possible states of combined system. The states that can not be written as (5), are called *entangled*.

For a pair of r and s-qudits it is useful to represent the density matrix in the so-called Fano form [19, 20]:

$$\varrho = \frac{1}{rs}\left(\mathbb{I}_{rs} + \sum_{i=1}^{r^2-1} a_i \, \lambda_i \otimes \mathbb{I}_s + \sum_{i=1}^{s^2-1} b_i \, \mathbb{I}_r \otimes \tau_i + \sum_{i=1}^{r^2-1}\sum_{j=1}^{s^2-1} c_{ij}\lambda_i \otimes \tau_j\right) . \tag{6}$$

In (6) matrices λ_i and τ_i are basis elements of the su(r) and su(s) algebras respectively. The real $(r^2-1)\times(s^2-1)$ matrix $C = ||c_{ij}||$ is so-called *"correlation matrix"*. Meaning of parameters $\boldsymbol{a} = (a_1, \dots, a_{r^2-1})$ and $\boldsymbol{b} = (b_1, \dots, b_{s^2-1})$ becomes clear after performing the partial trace operation [5]:

$$\varrho^{(A)} := \mathrm{Tr}_B(\varrho) = \frac{1}{r}(\mathbb{I}_r + \boldsymbol{a}\cdot\boldsymbol{\lambda})\,, \qquad \varrho^{(B)} := \mathrm{Tr}_A(\varrho) = \frac{1}{s}(\mathbb{I}_s + \boldsymbol{b}\cdot\boldsymbol{\tau}).$$

The vectors $\boldsymbol{a}$ a $\boldsymbol{b}$ are Bloch vectors for subsystems whose states are describing by matrices $\varrho^{(A)}$ and $\varrho^{(B)}$, respectively.

The entanglement properties of density matrices (6) as well as more general multipartite systems admit formulation in terms of invariants of the so-called local groups [9]. In the next paragraph the corresponding notions will be introduced.

3 The entanglement space

3.1 The local invariance

On the space of density matrices of n-level system the group SU(n) acts in adjoint manner

$$\varrho \quad \to \quad \varrho' = U^\dagger \varrho \, U\,. \tag{7}$$

If a quantum system is obtained by combining r-subsystems with $n_1, n_2, \ldots, n_r$ levels, the non-local properties of the resulting composite system can be put into a correspondence with a certain decomposition of the unitary operations in (7). Namely, from all unitary actions we separate the group of so-called *local unitary transformations* (LUT)

$$\mathrm{SU(n_1)} \otimes \mathrm{SU(n_2)} \otimes \cdots \otimes \mathrm{SU(n_r)}\,, \tag{8}$$

acting independently on the density matrices of each subsystems

$$\varrho^{(n_i)} \quad \to \quad \varrho^{(n_i)\prime} = g^\dagger \varrho^{(n_i)}\, g \qquad g \in \mathrm{SU(n_i)}\,, \quad i = 1, 2, \ldots, r\,.$$

Two states of composite system connected by the LUT transformations (8) have the same non-local properties. The latter can be changed only by the rest of the unitary actions

$$\frac{\mathrm{SU(n)}}{\mathrm{SU(n_1)} \otimes \mathrm{SU(n_2)} \otimes \cdots \otimes \mathrm{SU(n_r)}}\,, \qquad n = \prod_{i=1}^{r} n_i\,,$$

generating the class of non-local transformations.

As it was mentioned in the Introduction the action of LUT is not transitive. The equivalence of states regarding the action (8) gives rise to a decomposition of the space of matrices into the equivalence classes (orbits). The union of these classes, i.e., the orbit space, is customary to call as the "entanglement space" $\mathcal{E}_n$.

3.2 Orbit space and local polynomial invariants

The main motivation for studying of $\mathcal{E}_n$ is necessity to work out qualitative criteria and quantitative measures for characterization of non-locality in composite systems [6, 12].

As it was mentioned above, a canonical method for description of the orbit space $\mathcal{E}_n$ is the theory of classical invariants [11]. Within this approach, starting from the works by Linden and Popescu [9], series of interesting results, which clarify the mathematical contents of the entanglement phenomenon, has been obtained. A considerable progress was achieved for pure states. As an example, we refer here to the construction of Hilbert series for a multipartite systems of qubits [21] and classification of pure entangled states based on the theory of hyperdeterminants [22].

Analysis of the orbit space for systems in mixed states is much more vague. The generic questions of construction of basis for rings of local invariants for mixed states have been considered in [13, 14]. With this aim the algorithmic methods of computer algebra were used [23], [24].[3]

According to the theory of invariants [11], the ring of polynomial invariants $\mathbb{C}[V]^G$, of linear space V over the complex numbers $\mathbb{C}$, under the action of a group G, represents the graded algebra

$$\mathbb{C}[V]^G = \bigoplus_{k=1}^{\infty} A_k,$$

where A_k is the space of homogeneous G-invariant polynomials of degree k.

The special unitary groups SU(n) belong to the reductive algebraic groups. Their ring is finitely generated [11], and $\mathbb{C}[V]^G$ is Cohen-Macaulay type [26]. However, straightforward application of this construction to the problems of quantum entanglement is complicated by the fact that the space $\mathfrak{P}_+$, on which the local group (8) acts is not a linear space. As it was already emphasized in the Introduction, density matrices are the positive semi-definite and therefore the space of representations $\mathfrak{P}_+$ is nonlinear semi-definite algebraic manifold. Bellow we suggest the trick how to overcome this difficulty, exemplifying the problem in details for a system of pair of qubits.

Let start with the construction of the ring $\mathbb{C}[\,\mathcal{H}_{4\times4}\,]^{\mathrm{SU(2)\otimes SU(2)}}$ of the adjoint action invariants on the space of 4×4 Hermitian matrices $\mathcal{H}_{4\times4}$. In order to define the ring $\mathbb{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU(2)\otimes SU(2)}}$, note that the space of positive-definite matrices $\mathfrak{P}_+$ is subspace of $\mathcal{H}_{4\times4}$, which is invariant under the action of $\mathrm{SU}(4)$. As we demonstrate below the subset $\mathfrak{P}_+$ admits representation via the set of polynomial inequalities [4]

$$P_a(\mathfrak{C}_2, \mathfrak{C}_3, \mathfrak{C}_4) \geq 0\,, \qquad a = 1, 2, 3 \tag{9}$$

in three invariants, $\mathfrak{C}_2, \mathfrak{C}_3$ and $\mathfrak{C}_4$, of the enveloping algebra of SU(4) group. From the other side, since $\mathfrak{C}_2, \mathfrak{C}_3, \mathfrak{C}_4$ are at the same time invariants of $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$, then it is possible to construct in $\mathbb{C}[\,\mathcal{H}_{4\times4}\,]^{\mathrm{SU(2)\otimes SU(2)}}$ such

[3]Unfortunately, applications of the existing algorithmic methods, including the Gröbner bases technique, to the analysis of the ring of polynomial invariants for multipartite systems is not effective due to the sharp growth of the number of algebraic operations with the increasing number of qubits.

[4]One can find a description of $\mathfrak{P}_+$, similar to the given here, in [27, 28, 29].

a basis that includes these invariants. As result, having this basis and taking into account the inequalities (9), we will be able to characterize the ring $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU(2)}\otimes\mathrm{SU(2)}}$ completely. According to the consideration given in the subsequent paragraphs a basis of the ring can be chosen in a way that only the primary invariants of degree 2, 3 and one secondary invariant of degree 4 presented in the ring's Hironaka decomposition [11] are constrained by the above polynomial inequalities (9).

4 Non-negativity of density matrix

To succeed in our program of construction of an optimal homogeneous basis for the ring $\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU(2)}\otimes\mathrm{SU(2)}}$ let us start with the discussion of positive semi-definiteness of density matrices. Below the requirement of non-negativity will be formulated in the form of inequalities in invariants of the adjoint action of SU(n) group on $\mathfrak{P}_+$.

4.1 $\mathfrak{P}_+$ in terms of Casimirs of SU(n)

A Hermitian operator is positive semi-definite if and only if all its characteristic numbers are non-negative. The condition of non-negativity of Hermitian operator can be formulated solely in terms of coefficients of its characteristic equation:

$$|\mathbb{I}_n\, x - \varrho| = x^n - S_1 x^{n-1} + S_2 x^{n-2} - \ldots + (-1)^n S_n = 0\,. \qquad (10)$$

The coefficients S_k in (10) are given as the sums of principal minors of k-th order:

$$S_k = \sum_{1\leq i_1<\ldots<i_k\leq n} \varrho\begin{pmatrix} i_1 & \ldots & i_k \\ i_1 & \ldots & i_k \end{pmatrix}\,, \qquad k = 1, \ldots, n.$$

Since the matrix ϱ is Hermitian all its characteristic numbers x_k are real roots of the characteristic equations (10). When x_k are positive then all S_k being the symmetric polynomials

$$S_k = \sum_{1\leq i_1\leq\ldots\leq i_k\leq n} \prod_{j=1}^{k} x_{i_j}\,,$$

are non-negative real numbers. The inverse statement is true as well; the non-negativity of the coefficients S_k provides the non-negativity of roots x_k.

The Descartes theorem [30]: a number of positive roots (taking into account their multiplicity) equals to the number of signs changes in the sequence of the coefficients of the polynomial equation, gives proof of this observation (see e.g. [27]).

So, non-negativity of density matrices can be written in the invariant way as condition of non-negativity of the coefficients of its characteristic equation:

$$S_k \geq 0\,, \qquad k = 1, \ldots, n. \tag{11}$$

We give here, for further use, the explicit form of a few first coefficients S_k, written in terms of n-dimensional Bloch vector $\boldsymbol{\xi}$ [27, 28]:

$$\begin{aligned}
S_2 &= \frac{1}{2!}\frac{n-1}{n}\,(1-\boldsymbol{\xi}\cdot\boldsymbol{\xi}),\\
S_3 &= \frac{1}{3!}\frac{(n-1)(n-2)}{n^2}\,(1-3\,\boldsymbol{\xi}\cdot\boldsymbol{\xi}+2\,(\boldsymbol{\xi}\vee\boldsymbol{\xi})\cdot\boldsymbol{\xi}),\\
S_4 &= \frac{1}{4!}\frac{(n-1)(n-2)(n-3)}{n^3}\,(1-6\,\boldsymbol{\xi}\cdot\boldsymbol{\xi}+8\,(\boldsymbol{\xi}\vee\boldsymbol{\xi})\cdot\boldsymbol{\xi}\\
&\quad +3\,\frac{n-1}{n-3}(\boldsymbol{\xi}\cdot\boldsymbol{\xi})^2-6\,\frac{n-2}{n-3}(\boldsymbol{\xi}\vee\boldsymbol{\xi})\cdot(\boldsymbol{\xi}\vee\boldsymbol{\xi})).
\end{aligned}$$

Besides from the restrictions (11) there are upper bounds on S_k due to the normalization condition $\mathrm{Tr}(\varrho)=1\,,\ \ \mathrm{Tr}(\varrho^k)\leq 1\,$, for $k\geq 2\,$. Note, that the equality fulfils for pure states and the maximal values of S_k are achieved for the equal eigenvalues x_i of density matrices.

Finally, the positive semi-definiteness and normalizability conditions for density matrices of n-level system can be written as the following set of inequalities

$$0 \leq \frac{k!\,n^{k-1}\,S_k}{(n-1)(n-2)\ldots(n-k+1)} \leq 1\,, \qquad\qquad k = 2, \ldots, n. \tag{12}$$

Coefficients $S_k,\ k=1,\ldots,n$ of the characteristic equation are invariants under the adjoint action of $\mathrm{SU(n)}$ group. They are algebraically independent and can be represented via polynomials in the Casimir operators of the corresponding enveloping algebra. Below, the case $n=4\,$, related to the system of 2-qubits, is considered in details and inequalities (12) are rewritten directly in terms of the Casimir operators of the enveloping $\mathrm{su}(4)$ algebra.

4.2 Restrictions on invariants of SU(4)

The group SU(4) has three Casimir operators whose expressions in terms of the components of 15-dimensional Bloch vector $\boldsymbol{\xi}$ (see the decomposition (3)) can be written as

$$\mathfrak{C}_2 = \boldsymbol{\xi} \cdot \boldsymbol{\xi} \,, \tag{13}$$
$$\mathfrak{C}_3 = \boldsymbol{\xi} \vee \boldsymbol{\xi} \cdot \boldsymbol{\xi} \,, \tag{14}$$
$$\mathfrak{C}_4 = \boldsymbol{\xi} \vee \boldsymbol{\xi} \cdot \boldsymbol{\xi} \vee \boldsymbol{\xi} \,. \tag{15}$$

Because for an arbitrary 4-level system the coefficients S_2, S_3 and S_4 of characteristic equation of density matrix are expressible via these Casimir operators

$$\begin{aligned} S_2 &= \frac{3}{8}(1 - \mathfrak{C}_2)\,, \\ S_3 &= \frac{1}{16}(1 - 3\mathfrak{C}_2 + 2\mathfrak{C}_3)\,, \\ S_4 &= \frac{1}{256}((1 - 3\mathfrak{C}_2)^2 + 8\mathfrak{C}_3 - 12\mathfrak{C}_4)\,, \end{aligned}$$

the set (12) reduces to the following constraints on SU(4) invariants

$$\begin{gathered} 0 \leq \mathfrak{C}_2 \leq 1\,, \\ 0 \leq 3\mathfrak{C}_2 - 2\mathfrak{C}_3 \leq 1\,, \\ 0 \leq (1 - 3\mathfrak{C}_2)^2 + 8\mathfrak{C}_3 - 12\mathfrak{C}_4 \leq 1\,. \end{gathered} \tag{16}$$

In the space spanned by invariants $\mathfrak{C}_2, \mathfrak{C}_3$ and $\mathfrak{C}_4$ inequalities (16) define the bounded domain depicted on the Figure 1.

5 The ring of local invariants $\mathbb{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes \mathrm{SU}(2)}$

Consider the density matrix of two qubits parameterized in the Fano form:

$$\varrho = \frac{1}{4}\left[\,\mathbb{I}_2 \otimes \mathbb{I}_2 + \boldsymbol{a}\cdot\boldsymbol{\sigma} \otimes \mathbb{I}_2 + \mathbb{I}_2 \otimes \boldsymbol{b}\cdot\boldsymbol{\sigma} + c_{ij}\,\sigma_i \otimes \sigma_j\,\right], \tag{17}$$

where 3-component vectors $\boldsymbol{a} = (a_1, a_2, a_3)$ and $\boldsymbol{b} = (b_1, b_2, b_3)$ are Bloch vectors of constituent qubits, $\sigma_i\,,\ i = 1, 2, 3$ - the Pauli matrices making up the basis of algebra su(2):

$$\sigma_1 = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}, \quad \sigma_2 = \begin{pmatrix} 0 & -i \\ i & 0 \end{pmatrix}, \quad \sigma_3 = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}. \tag{18}$$

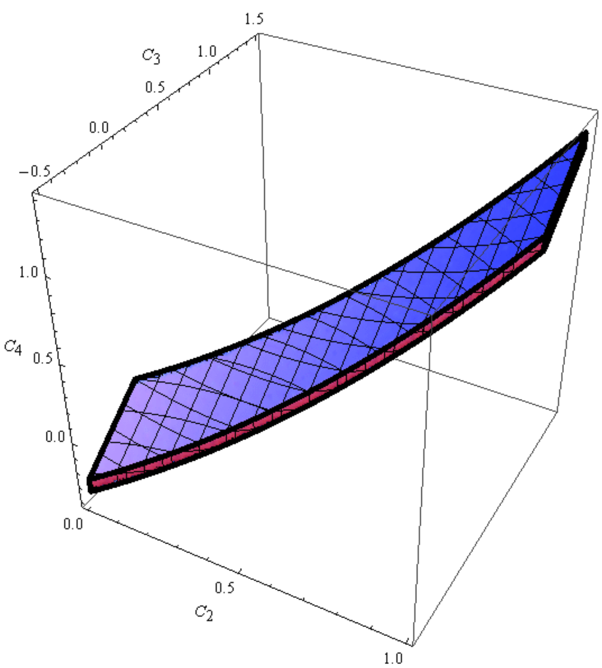

Figure 1: The allowed region for the values of Casimirs $\mathfrak{C}_2, \mathfrak{C}_3$ and $\mathfrak{C}_4$.

The correlation matrix C of pair of qubits has 9 elements $c_{ij}\ \ i,j=1,2,3$.

At first, following our program of the construction of the ring of invariants $\mathbb{C}[\,\mathfrak{P}\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ outlined in paragraph 3.2, we identify the space of parameters $\boldsymbol{a}\,,\boldsymbol{b}$ and C with $\mathbb{R}^{15}$, ignoring for a moment all restrictions due to the non-negativity of density matrices. Apart from this we linearize the adjoint action (7) of the local group $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$

$$V_A \ \to\ V'_A = L_{AB}V_B \qquad A,B=1,\dots,15\,, \tag{19}$$

with 15×15 matrix $L\in \mathrm{SU}(2)\otimes\mathrm{SU}(2)\otimes\overline{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$.

So, our preliminary issue is to build up the ring of polynomial invariants of linear action of $\mathrm{SU}(2)\otimes\mathrm{SU}(2)\otimes\overline{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ group on the linear space $\mathbb{R}^{15}$. Note that the linearization (19) allows to use the prompt from the Molien formula for the generating function of invariants for π_G representations of a compact group G [24]:

$$M(q)=\int_G \mathrm{d}\mu_G\,\frac{1}{\det||\mathrm{id}-q\pi_G||}\,, \tag{20}$$

where the integral is taken over the group G with the Haar measure $\mathrm{d}\mu_G$.

The Molien function provides information on the polynomial invariants ring's structure. Firstly, its formal series in powers of parameter q, the so-called Hilbert-Poincare series:

$$M(q)=\sum_{k\geq 0} d_k q^k \ \in\ \mathbb{Z}[q]\,,$$

points out the dimension, d_k, of the space of homogeneous invariants of degree k. Secondarily, being a rational function, (20) admits (non-uniquely) for $q<1$, the representation

$$M(q)=\frac{\sum_{k=0}^r q^{\deg J_k}}{\Pi_{m=1}^n(1-q^{\deg K_m})}\,,$$

From this form of the Molien function on can conclude on the number and order of the primary $K_i\,,\ i=1,2,\dots,n$, and secondary $J_i\,,\ i=1,2,\dots,r$, invariants of the Cohen-Macaulay algebra

$$\mathbb{C}[V]^G=\bigoplus_{k=0}^r\, J_k\,\mathbb{C}[K_1,K_2,\dots,K_n]\,.$$

As computations show, the Molien function for mixed states of two qubits can be written as [13, 14]:

$$M(q) = \frac{1+q^4+q^5+3q^6+2q^7+2q^8+3q^9+q^{10}+q^{11}+q^{15}}{(1-q)(1-q^2)^3(1-q^3)^2(1-q^4)^3(1-q^6)}\,, \tag{21}$$

According to the result (21), a basis of ring consists from 10 primary invariants of degree $1,2,2,2,3,3,4,4,4,6$ and 15 secondary invariants of degree $4,5,6,6,6,7,7,8,8,9,9,9,10,11,15\,.$

More detailed information on invariants dependence on coefficients of the decomposition (17) can be extracted using the so-called method of many-parametric generating functions [24]. In our case the many-parametric generating function depends not only on one parameter q, but is a function of three arguments, $F(a,b,c)$. The contribution from variables $\boldsymbol{a}\,,\boldsymbol{b}$ and c_{ij} into the Molien function now is taken with the weights determined by each independent parameter, $a\,,b$ and c respectively.

It is worth to note that the generating function $F(a,b,c)$ was found already in the middle of 70-th of the last century [31, 32], in connection with so-called problem of *"missing index"* which arose within issue of nuclei spectrum classification. The corresponding mathematical formulation and solution of the problem can be found, e.g., in [31]. Further, in our presentation, we will mainly follow the article [32].

Consider the space of all polynomials in fifteen variables a_i, b_i and c_{ij} $i,j=1,2,3$. In virtue of the adjoint action of the local group the space of Bloch's parameters is decomposed into the irreducible representations of the $\mathrm{SO}(3)\otimes\mathrm{SO}(3)$ group. More precisely, the variables a_i, b_i and c_{ij} are transformed according to the representations $D_1\times D_0$, $D_0\times D_1$, and $D_1\times D_1$ correspondingly. Since the subspace, $P_{s,t,q}[a_i,b_i,c_{ij}]$, of homogeneous polynomials in variables a_i, b_i, c_{ij} of degree s,t,q correspondingly, is invariant under the action $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$, all invariants C can be classified according to their degrees of homogeneity, i.e., $C^{(s\,t\,q)}$.

Consider, following the construction suggested in [32], the set of invariants:[5]

3 invariants of second degree

$$C^{(002)} = c_{ij}c_{ij}\,,\quad C^{(200)} = a_ia_i\,,\quad C^{(020)} = b_ib_i\,, \tag{22}$$

[5]Below, everywhere it is assumed the summation over all repeated indices from one to three.

2 invariants of third degree

$$C^{(003)} = \frac{1}{3!}\epsilon_{ijk}\epsilon_{\alpha\beta\gamma}c_{i\alpha}c_{j\beta}c_{k\gamma}\,, \qquad C^{(111)} = a_i c_{ij} b_j\,, \tag{23}$$

4 invariants of fourth degree

$$\begin{aligned} C^{(004)} &= c_{i\alpha}c_{i\beta}c_{j\alpha}c_{j\beta}\,, && (24)\\ C^{(202)} &= a_i a_j c_{i\alpha}c_{j\alpha}\,, && (25)\\ C^{(022)} &= b_\alpha b_\beta c_{i\alpha}c_{i\beta}\,, && (26)\\ C^{(112)} &= \epsilon_{ijk}\epsilon_{\alpha\beta\gamma}a_i b_\alpha c_{j\beta}c_{k\gamma}\,, && (27) \end{aligned}$$

1 invariant of fifth degree

$$C^{(113)} = a_i c_{i\alpha}c_{j\alpha}c_{j\beta}b_\beta\,, \tag{28}$$

4 invariants of sixth degree

$$\begin{aligned} C^{(123)} &= \epsilon_{ijk}b_i c_{\alpha j}a_\alpha c_{\beta k}c_{\beta l}b_l\,, && (29)\\ C^{(204)} &= a_i c_{i\alpha}c_{j\alpha}c_{j\beta}c_{k\beta}a_k\,, && (30)\\ C^{(024)} &= b_i c_{\alpha i}c_{\alpha j}c_{\beta j}c_{\beta,k}b_k\,, && (31)\\ C^{(213)} &= \epsilon_{\alpha\beta\gamma}a_\alpha c_{\beta i}b_i c_{\gamma j}c_{\delta j}a_\delta\,, && (32) \end{aligned}$$

2 invariants of seventh degree

$$\begin{aligned} C^{(214)} &= \epsilon_{ijk}b_i c_{\alpha j}a_\alpha c_{\beta k}c_{\beta l}c_{\gamma l}a_l\,, && (33)\\ C^{(124)} &= \epsilon_{\alpha\beta\gamma}a_\alpha c_{\beta j}b_j c_{\gamma k}c_{\delta k}c_{\delta l}b_l\,, && (34) \end{aligned}$$

2 invariants of eighth degree

$$\begin{aligned} C^{(125)} &= \epsilon_{ijk}b_i c_{\alpha j}c_{\alpha l}b_l c_{\beta k}c_{\beta m}c_{\gamma m}a_\gamma\,, && (35)\\ C^{(215)} &= \epsilon_{\alpha\beta\gamma}a_\alpha c_{\beta i}c_{\delta i}a_\delta c_{\gamma k}c_{\varrho k}c_{\varrho l}b_l\,, && (36) \end{aligned}$$

2 invariants of ninth degree

$$\begin{aligned} C^{(306)} &= \epsilon_{\alpha\beta\gamma}a_\alpha c_{\beta i}c_{\delta i}a_\delta c_{\gamma j}c_{\varrho j}c_{\varrho k}c_{\sigma k}a_\sigma\,, && (37)\\ C^{(036)} &= \epsilon_{ijk}b_i c_{\alpha j}c_{\alpha l}b_l c_{\beta k}c_{\beta m}c_{\gamma m}c_{\gamma s}b_s\,, && (38) \end{aligned}$$

From these invariants the basis of $\mathbb{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ can be build. As the criterion of its construction we choose the principle of usage of basis with the minimal number of elements involved in the definition of $\mathfrak{P}_+$. Having in mind this rule and noting that the space $\mathfrak{P}_+$ is defined in terms of the Casimir operators of SU(4) group (13)-(15), we expand $\mathfrak{C}_2, \mathfrak{C}_3, \mathfrak{C}_4$ over the set of above introduced local invariants (22)-(24):

$$\mathfrak{C}_2 = \frac{1}{3}\,(C^{(200)} + C^{(020)} + C^{(002)})\,, \tag{39}$$

$$\mathfrak{C}_3 = C^{(111)} - C^{(003)}\,, \tag{40}$$

$$\mathfrak{C}_4 = \frac{1}{6}\,[2(C^{(200)}C^{(020)} + C^{(202)} + C^{(022)} - C^{(112)}) + (C^{(002)})^2 - C^{(004)}]\,. \tag{41}$$

From equations (39)-(41) it follows that one can consider the Casimir operators $\mathfrak{C}_2, \mathfrak{C}_3, \mathfrak{C}_4$ as the basis elements instead of scalars $C^{(002)}, C^{(003)}$ and $C^{(112)}$.

Bear in mind this observation and using the results of [14], where the ring $\mathbb{C}[\,\mathbb{R}^{16}\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$ was described, we define the following set consisting from 10 *primary invariants*, including the Casimir operators $\mathfrak{C}_2, \mathfrak{C}_3$,

$$\begin{array}{lll}
\deg = 4\,, & K_1 = 1\,, & \\
\deg = 2\,, & K_2 = \mathfrak{C}_2\,, & K_3 = C^{(200)}\,, \quad K_4 = C^{(020)}\,, \\
\deg = 3\,, & K_5 = \mathfrak{C}_3\,, & K_6 = C^{(111)}\,, \\
\deg = 4\,, & K_7 = C^{(004)}\,, & K_8 = C^{(202)}\,, \quad K_9 = C^{(022)}\,, \\
\deg = 6\,, & K_{10} = C^{(204)} + C^{(024)}\,, &
\end{array} \tag{42}$$

and 15 *secondary invariants* including the Casimir $\mathfrak{C}_4$

$$\begin{array}{lll}
\deg = 4\,, & J_1 = \mathfrak{C}_4\,, & \\
\deg = 5\,, & J_2 = C^{(113)}\,, & \\
\deg = 6\,, & J_3 = C^{(204)} - C^{(024)}\,, & J_8 = C^{(123)}\,, \quad J_9 = C^{(213)}\,, \\
\deg = 7\,, & J_{10} = C^{(214)}\,, & J_{11} = C^{(124)}\,, \\
\deg = 8\,, & J_{12} = C^{(215)}\,, & J_{13} = C^{(125)}\,, \\
\deg = 9\,, & J_4 = J_1 J_2\,, & J_{14} = C^{(306)}\,, \quad J_{15} = C^{(036)}\,, \\
\deg = 10\,, & J_5 = J_1 J_3\,, & \\
\deg = 11\,, & J_6 = J_2 J_3\,, & \\
\deg = 15\,, & J_7 = J_1 J_2 J_3\,. &
\end{array} \tag{43}$$

We conclude that the set of homogeneous invariants (42)-(43) represents the basis for the ring $\mathbb{C}[\,\mathfrak{P}\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$:

$$\mathbb{C}[\mathfrak{P}_+]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)} = \bigoplus_{k=0}^{15} J_k\,\mathbb{C}[K_1, K_2, \dots, K_{10}]\,,$$

under the condition, that two primary invariants K_2, K_5 and one secondary invariant J_1 satisfy the inequalities (16).

6 Conclusion

An essential issue of the quantum theory of information is qualitative and quantitative characterization of purely quantum correlations caused by the entanglement of quantum states. Theory of classical invariants provides tools for studies of the corresponding space of entanglement, i.e., the orbit space of action of the group of local transformations on the space of states of composite systems. For the case we are interesting in, system of two qubits in a mixed state, the local transformations of the density matrices form the $\mathrm{SU}(2)\otimes\mathrm{SU}(2)$ group. Its adjoint action, on the space of the Hermitian, unit trace matrices, identified with $\mathbb{R}^{15}$, defines the principal orbit space

$$\mathcal{O} := \frac{\mathbb{R}^{15}}{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}\,,$$

with dimension

$$\dim\mathcal{O} = 15 - 2\times 3 = 9.$$

However, the orbit space defined in such a way is not the space of entanglement $\mathcal{E}_2$. Due to the non-negativity of density matrices the space of physical states is $\mathfrak{P}_+\subset\mathbb{R}^{15}$. In the present article we suggest the description of $\mathfrak{P}_+$ based on the polynomial inequalities in Casimir operators of the enveloping algebra $\mathrm{su}(4)$. Furthermore, we show how these restrictions can be effectively taken into account constructing the basis for the ring $\mathbb{C}[\,\mathfrak{P}_+\,]^{\mathrm{SU}(2)\otimes\mathrm{SU}(2)}$, provided for the Hironaka decomposition with only two primary invariants of degree 2, 3 and one secondary invariant of degree 4 constrained by the polynomial inequalities (16).

Concluding it is important to emphasize that without the inequalities (16), the usage of local invariants for “coordinatization” of the space of entanglement $\mathcal{E}_2$ is not correct. We leave for a future publications analysis of those constraints consequences on the geometry of $\mathcal{E}_2\subset\mathcal{O}$.

Acknowledgments

This work was supported in part the Georgian National Science Foundation research grant GNSF/ST08/4-405 and by the Russian Foundation for Basic Research (grant No. 10-01-00200) and by the Ministry of Education and Science of the Russian Federation (grant No. 3810.2010.2).

References

[1] A. Einstein, B. Podolsky and N. Rosen, Can quantum-mechanical description of physical reality be considered complete?, Phys. Rev. **47** (1935), 777–780.

[2] J. Bell. *Speakable and Unspeakable in Quantum Mechanics,* Cambridge University Press, Cambridge, 1987.

[3] A. Aspect. Bell's theorem: the naiv view of an experimentalist. In: *Quantum [Un]speakables: From Bell to Quantum Information*, R.A. Bertlmann and A. Zeilinger (Eds.), Springer Verlag, Berlin, 2002.

[4] M.A. Nielsen and I.L. Chuang,*Quantum Computation and Quantum Information*, Camridge University Press, 2000.

[5] V.Vedral, *Introduction to Quantum Information Science*, Oxford University Press, New York, 2006.

[6] I. Bengtsson and K. Źyczkowski, *Geometry of Quantum States. An Introduction to Quantum Entanglement,* Cambridge University Press, 2006.

[7] R.F. Werner, Quantum states with Einstein-Podolski-Rosen correlations admitting a hidden-variable model, Phys. Rev. A **40** (1989), 4277.

[8] J. Schlienz and G. Mahler, Description of entanglement, Phys.Rev. A **52** (1995), 4396–4404.

[9] N. Linden and S. Popescu, On multi-particle entanglement, Fortschr. Phys. **46** (1998), 567–578.

[10] H. Weyl, *The Classical Groups: Their Invariants and Representations*, Princeton University Press, 1939.

[11] V.L. Popov and E.B. Vinberg, *Invariant theory*, in Algebraic Geometry IV, Encycl. Math. Sci., Vol.55, Springer-Verlag, 123-273, 1994.

[12] M. Kus and K. Źyczkowski, Geometry of entangled states, Phys. Rev. A **63** (2001), 032307 [13 pages].

[13] M. Grassl, M. Rötteler, and T. Beth, Computing local invariants of qubit systems, Phys. Rev. A 58 (1998), 1853–1856.

[14] R.C. King, T.A. Welsh and P.D. Jarvis, The mixed two-qubit system and the structure of its ring of local invariants, J. Phys. A: Math. Theor. **40** (2007), 10083–10108.

[15] J. von Neumann, Warscheinlichtkeitstheoritischer aufbau der Quantemechanik, Göttingen Nachrichten, (1927), 245–272.

[16] L.D. Landau, Das dämpfungsproblem in der Wellenmechanik, Zeitschrift für Physik, **45** (1927), 430–441.

[17] K. Blum, *Density Matrix. Theory and Applications*, Plenum Press, New York, 1981.

[18] F.T. Hioe and J.H. Eberly, $N-$Level Coherence Vector and Higher Conservation Laws in Quantum Optics and Quantum Mechanics. Phys. Rev. Lett. **47** (1981), 838–841.

[19] U. Fano, Description of states in quantum mechanics by density matrix and operator techniques. Rev. Mod. Phys. **29** (1957), 74–93.

[20] U. Fano, Pairs of two-level systems. Rev. Mod. Phys. **55** (1983), 855–874.

[21] J.-G. Luque and J.-Y. Thibon, The polynomial invariants of four qubits. Phys. Rev. A **63** (2003), 042303 [5 pages].
J.-G. Luque and J.-Y. Thibon, Algebraic invariants of five qubits. J. Phys. A: Math. Gen. **39** (2005), 371–377.

[22] A. Miyake, Classification of multipartite entangled states by multidimensional determinants, Phys. Rev. A **67** (2003), 012108 [10 pages].

[23] B. Sturmfels, *Algorithms in Invariant Theory*. Springer-Verlag, Wien, 1993.

[24] H. Derksen and G. Kemper, *Computational Invariant Theory*, Encyclopedia of Mathematical Sciences, vol. 130, Springer-Verlag, Berlin, 2002.

[25] B. Buchberger, Gröbner bases – an algorithmic method in polynomial ideal theory, in: N.K. Bose (ed.): *Multidimensional Systems Theory*, D. Reidel, Dordrecht, (1985), 184–232.

[26] M. Hochster and J. Roberts, Rings of invariants of reductive groups acting on regular rings are Cohen-Macaulay, Advances in Mathematics **13** (1974), 125–175.

[27] G Kimura, The Bloch vector for N-level systems, Phys. Lett. A **314**, (2003), 339–349,

[28] M.S. Byrd and N. Khaneja, Characterization of the positivity of the density matrix in terms of the coherence vector representation, Phys. Rev. A**68** (2003), 062322 [13 pages].

[29] S. Kryszewski and M. Zachcial, Positivity of the N$\times$ N density matrix expressed in terms of polarization operators, J.Phys.A: Math. Theor. **39** (2006), 5921–5931.

[30] E.B. Vinberg, *A Course in Algebra*, (Graduate Studies in Mathematics, vol. 56) AMS 2003.

[31] B.R. Judd, W. Miller Jr., J. Patera and P. Winternitz, Complete set of commuting operators and O(3) scalars in the enveloping algebra of SU(3), J. Math. Phys., **15** (1974), 1787–1799.

[32] C. Quesne, SU(2)$\otimes$ SU(2) scalars in the enveloping algebra of SU(4), J. Math. Phys. **17** (1976), 1452–1467.